CLAIMS

1. A process for secure communication over a wireless network (NCA) including a group of terminals (T), wherein such terminals (T) exchange information ciphered by means of at least one key, characterized in that it includes the step of generating said at least one key independently at each said terminal (T) in said group by means of a protocol of the group key agreement (GKAP) type.

2. The process of claim 1, characterized in that it includes the steps of:

- generating, at each said terminal (T) in said group, respective secret local data and maintaining said local data secret at said terminal (T),
- exchanging publicly accessible information among the terminals (T) in said group, and
- generating, independently at each said terminal (T) in the group, said at least one key on the basis of said respective local data maintained secret at each said terminal (T) and said publicly accessible information.

3. The process of claim 2, characterized in that it includes the step of incorporating to said publicly accessible information coded information representative of each terminal (T) in said group, whereby generation of said at least one key is contributed by all the terminals (T) in said group.

4. The process of claim 3, characterized in that it includes the steps of:

- encoding each terminal (T) in said group by means of a respective labels,
- generating a vector of the labels of all the terminals (T) in said group, wherein said vector is included in said publicly accessible information exchanged among the terminals (T) in said group.

5. The process of claim 2, characterized in that publicly accessible information exchanged among terminals in said group is representative of a tree-structure for generating said at least one key.

6. The process of claim 1, characterized in that it includes the step of generating said at least one key independently at each said terminal (T) in said group by means of a Diffie-Hellman group algorithm.

7. The process of claim 6, characterized in that said algorithm is the TGDH algorithm.

8. The process of claim 1, characterized in that it includes the step of each terminal (T) in said group authenticating itself by means of digital authentication information.

9. The process of claim 8, characterized in that it includes the step of each terminal (T) in said group authenticating itself by means of a digital certificate.

10. The process of claim 2, characterized in that it includes the step of exchanging said publicly accessible information by means of information packets.

11. The process of claim 10, characterized in that it includes the step of fragmenting said publicly accessible information over a plurality of information packets.

12. The process of claim 2, characterized in that it includes the steps of each terminal (T) in said group authenticating itself by means of digital authentication information, fragmenting said publicly accessible information over a plurality of information packets and associating said authentication information with all of said packets.

13. The process of claim 2, characterized in that it includes the steps of each terminal (T) in said group authenticating itself by means of digital authentication information, fragmenting said publicly

accessible information over a plurality of information packets and including said digital authentication information with one of said packets, whereby the remaining part of said plurality of packets comprises a lower protocol layer conveying information resulting from said fragmentation.

14. The process of claim 1, characterized in that it includes the step of configuring said each terminal (T) in said group for generating at least one message selected out of the group consisting of:

- a join message generated when said terminal (T) enters said group and conveying information that merged with other information provided by all the other terminals (T) in said group is adapted to generate said at least one key;

- a key message generated during the generation of said at least one key and containing data that respective terminal (T) other than a new terminal (T) joining said group have to provide for generating said at least one key, and

- a leave message generated to notify the other terminals in said group that the source terminal (T) is leaving the group.

15. The process of claim 1, characterized in that, when a new terminal (T) joins said group, it includes the step of selecting one of the other terminals (T) in the group for exchanging said publicly accessible information with said new terminal (T) joining the group.

16. A wireless network for secure communication among a group of terminals (T), wherein such terminals (T) exchange information ciphered by means of at least one key, characterized in that the terminals (T) in said group are configured for generating said at least one key independently at each terminal by means of a protocol of the group key agreement (GKAP) type.

17. The network of claim 16, characterized in that the terminals (T) in said group are configured for:

- generating, at each said terminal (T) in said group, respective secret local data and maintaining said local data secret at said terminal (T),

- exchanging publicly accessible information among the terminals (T) in said group, and

- generating, independently at each said terminal (T) in the group, said at least one key on the basis of said respective local data maintained secret at each said terminal (T) and said publicly accessible information.

18. The network of claim 17, characterized in that the terminals (T) in said group are configured for incorporating to said publicly accessible information coded information representative of each terminal (T) in said group, whereby generation of said at least one key is contributed by all the terminals (T) in said group.

19. The network of claim 17, characterized in that the terminals (T) in said group are configured for:

- encoding each terminal (T) in said group by means of a respective labels,

- generating a vector of the labels of all the terminals (T) in said group, wherein said vector is included in said publicly accessible information exchanged among the terminals (T) in said group.

20. The network of claim 17, characterized in that the terminals (T) in said group are configured for exchanging among them publicly accessible information representative of a tree-structure for generating said at least one key.

21. The network of claim 16, characterized in that the terminals (T) in said group are configured for generating said at least one key independently at each

said terminal (T) in said group by means of a Diffie-Hellman group algorithm.

22. The network of claim 21, characterized in that said algorithm is the TGDH algorithm.

23. The network of claim 16, characterized in that the terminals (T) in said group are configured for authenticating themselves by means of digital authentication information.

24. The network of claim 23, characterized in that the terminals (T) in said group are configured for authenticating themselves by means of a digital certificate.

25. The network of claim 17, characterized in that the terminals (T) in said group are configured for exchanging said publicly accessible information by means of information packets.

26. The network of claim 17, characterized in that the terminals (T) in said group are configured for fragmenting said publicly accessible information over a plurality of information packets.

27. The network of claim 17, characterized in that the terminals (T) in said group are configured for authenticating themselves by means of digital authentication information, fragmenting said publicly accessible information over a plurality of information packets and associating said authentication information with all of said packets.

28. The network of claim 17, characterized in that the terminals (T) in said group are configured for authenticating themselves by means of digital authentication information, fragmenting said publicly accessible information over a plurality of information packets and including said digital authentication information with one of said packets, whereby the remaining part of said plurality of packets comprises a

lower protocol layer conveying information resulting from said fragmentation.

29. The network of claim 16, characterized in that the terminals (T) in said group are configured for generating at least one message selected out of the group consisting of:

- a join message generated when said terminal (T) enters said group and conveying information that merged with other information provided by all the other terminals (T) in said group is adapted to generate said at least one key;

- a key message generated during the generation of said at least one key and containing data that respective terminal (T) other than a new terminal (T) joining said group have to provide for generating said at least one key, and

- a leave message generated to notify the other terminals in said group that the source terminal (T) is leaving the group.

30. The network of claim 16, characterized in that the terminals (T) in said group are configured for selecting, when a new terminal (T) joins said group, one the other terminals (T) in the group for exchanging said publicly accessible information with said new terminal (T) joining the group.

31. The network of claim 16, in the form of a network according to the 802.11 standard.

32. A computer program product, directly loadable in the memory of at least one computer and including software code portions adapted for implementing the method of any of claims 1 to 15.